**Komposition: Social Engineering, Denial-of-service attacks**

**Agenda:**

1. Forklar forskellige former for Social Engineering og hvordan sådanne forsøg kan detekteres
2. Forklar de mest almindelig DoS-angreb, og hvordan man kan minimere risikoen for at blive udsat for dette.

**Explain different ways to use Social Engineering (vectors)**

1. **Vishing**, også kaldet ”voice fishing”. En måde hvorpå man over telefonen forsøger at få adgang til personlige eller finansielle informationer og på den måde opnå en finansiel gevinst.

**Eksempel:**

* 1. En kriminel konfigurer en ”war dialer”, hvor der ringes til en række numre i en given region. Når en forbruger tager telefonen, vil en automatisk optagelse blive afspillet, som advarer forbrugeren om at deres kreditkort er blevet misbrugt, eller der har været usædvanlig aktivitet på deres bankkonto. Beskeden instruerer forbrugeren til omgående at ringe til et specifikt nummer. Når forbrugeren ringer nummeret op, vil vedkommende blive instrueret i at indtaste kreditkort nummer og bank nummer. Når dette er gjort, vil ”visher” nu have adgang til at misbruge kreditkortet eller have adgang til kontoen. Opkaldene er oftest brugt til at hente yderligere informationer, f.eks. PIN, udløbsdato, fødselsdag etc.

1. **Phishing,** også kaldet ”fishing”**.** Lidt ligesom vishing, forsøger den kriminelle at opbygge tillid, fx ved brug af spoofing, som får det til at ligne at man ringer fra samme virksomhed. I phishing opbygges tilliden på lignende vis, f.eks. ligner det at afsender skriver fra en e-mail, man kender.

”**Spear phishing**”, anvender meget brugerdefineret indhold, hvilket vil sige at de retter sig mod en specifik person. F.eks. en e-mail der referer til et køb der er sket fornyeligt.

”**Water holing**”, vil sige at de kriminelle retter sig mod en specifik gruppe, og forsøger at opnå viden om gruppens favorit sider, hvorefter de inficerer siderne med malware (f.eks. virus).

1. **Smishing,** er en kombination af ordet SMS og phishing. Det minder om phishing, men referer til skadelige beskeder sendt over SMS i stedet for e-mail. Disse beskeder er sendt, for at narre nogle til at give private informationer, f.eks. kodeord, CPR-nummer etc. Denne form er blevet en truende og voksende trussel indenfor verdens online sikkerhed.
2. **Impersonation,** også kendt som ”catfish”. Dette er nogle der udgiver sig for at være en anden, end den de er, eller kopiere en andens adfærd. Typisk er denne form for fishing, rettet mod en specifik person for at begå overgreb, bedrage eller svindle.

**Discuss ways to detect social engineering attempts (principles)**

* I e-mails kan et link se oprigtigt og troværdigt ud, men ved at hover henover, vil man kunne se det rigtige link, som der henvises til.
* Hvis en e-mail er sendt fra et offentligt email-domæne (f.eks. hotmail eller gmail). Ikke engang Google, vil sende e-mails fra disse domæner.
* Det er muligt at se om et opkald er spoofet, ved at sende en sms til brugeren med en kode han skal sige højt. På den måde kan man se han bruger den rigtige telefon. Eller man kan have en protokol for sikkerhedsspørgsmål, der tilknytter sig brugeren andre ikke kunne vide, fx info om hans konto i en bank, eller hans første hunds navn.
* Domænenavne er unikke og derfor vil en hacker godt kunne oprette et domæne der ligner et eksisterende domænenavn, men det ville aldrig kunne være identiske. (f.eks. **WORLD VVORLD** eller **IVORD NORD**).
* E-mailen er oftest dårligt skrevet eller tydeligt oversat gennem Google Translate.
* E-mailen indeholder oftest vedhæftede filer, som skal downloades eller links til loginsider, der beder om forbrugerens informationer.
* Indholdet i e-mailen vil oftest være desperat og give et indtryk for at være akut.

**Explain the most common DoS strategies**

* **Degradation of Service**, er en strategi hvor der er forsøges at forstyrre en websites hastighed og svartid, således at den enten er delvis eller permanent utilgængelig.
* **Denial of Service Level II, er et angreb,** som skal udløse en forsvarsmekanisme, der blokerer for det netværk segment, hvorfra angrebet kommer fra. I tilfælde af ”distributed attack” eller ”IP header modification”, vil det fuldt blokere det engrebede netværk fra internettet, dog uden at systemet bryder sammen.
* **Distributed Denial of Service DDoS**, er et angreb, der gør det umuligt for serveren at blackliste hele angrebet samtidig med at du kan lægge en stor server ned med mange små servere. Det forgår oftest ved at en hacker inficerer mange servere med malware f.eks. gennem Phishing e-mails. Forsøger man at lave et DDoS angreb, med en enkelt server vil de fleste servere meget hurtigt blackliste din ip. Serveren der udføre angrebet, skal være stærkere end den man forsøger at lægge ned.
* **HTTP POST DoS attack**, er et angreb hvor en hacker laver en forbindelse til en server, oftest med flere servere. Hver server laver en forbindelse med et højt tal i ”content-length header” i request. Dette gøres ved at sende et enkelt element (eller char) ad gangen, i stedet for at sende alt dataen samtidig. Den tid serveren er åben, vil blive nulstillet hver gang en ny element/char modtages, således vil den ende med at blive holdt åben rigtig længe.
* **Internet Control Message Protocol Attack**, er et ”Ping flood attack”, hvilket er en almindelig form for DoS angreb. Her vil en hacker forsøge på at overvælde en enhed eller en server med ICMP ”echo requests”, også kaldet pings. Normalt bruges pings til at diagnosticere tilstand og forbindelsesmulighed af en netværks enhed og forbindelsen mellem afsender og enheden. Ved at lave en overflod af pings til enheden, er netværket tvunget til at besvare disse pings med et tilsvarende antal pings (”echo responses”) , dette gør enheden utilgængelig for normal trafik.
* **Permanent DoS attacks phlashing**, denne form for angreb vil ødelægge den server der er angrebet, f.eks. ved at opdatere firmware.

**Discuss common means to minimize threads of DoS**

* For at minimere risikoen for DoS trusler, kan man bl.a.
  + sætte en firewall op.
  + sætte en proxy-server op.
  + huske at opdatere sine programmer.
  + sørge for at have udvidet bredbånd, så man kan tage imod flere requests.
  + lukke for port 53, for at undgå et forstærket DNS-server angreb.
  + installere et DoS-defense system (DDS).